UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,147	06/20/2001	Kristin E. Lauter	MS1-602US	5710

22801 7590 08/16/2005

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
KIM, JUNG W

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

17

Office Action Summary	**Application No.** 09/886,147	**Applicant(s)** LAUTER ET AL.	
	Examiner Jung W. Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) *1-10,12-16,18-22,24-28,30-37 and 39-47* is/are rejected.

7)☒ Claim(s) *11,17,23,29 and 38* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-47 are pending.

2. Applicant in the amendment filed on July 21, 2005 amended claims 20, 28, 34, 39, 40 and 45.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

4. The 112, second paragraph rejection to claim 39 is withdrawn as the amendment overcomes the rejection.

5. The 101 rejections to claims 20-39 are withdrawn as the amendment overcomes the 101 rejections.

Response to Arguments

6. The following is a response to Applicant's arguments on pgs. 16-29 in the amendment filed on July 21, 2005 (Remarks).

7. Applicant's arguments with respect to the 112, 1st paragraph rejections to claims 1-12, 14-19, 23, 29, 44 and 47 have been fully considered, and are persuasive; the 112, 1st paragraph rejections to these claims are withdrawn; however, after further

consideration, claims 1-10, 12-16 and 18-19 are rejected under 112, 2nd paragraph for omitting essential structural elements as outlined below.

8. Further, Applicant's arguments with respect to the 112, 1st paragraph rejections to claims 20-22, 24-28, 30-43 and 45-46 are not persuasive. Applicant alleges that the 112 rejections are not proper because the claimed invention is disclosed in the specification as required (see MPEP 2161.01(b)) (Remarks, pg. 16, last paragraph-pg. 17). In the case of the remaining rejected claims, the issue is not whether the specification includes an enabling disclosure, but whether the disclosure is enabling for the invention as recited in the claims ("As long as the specification discloses at least one method for making and using the claimed invention that bears a reasonable correlation to **the entire scope of the claim**, then the enablement of 35 U.S.C. 112 is satisfied", [emphasis added]); with respect to this issue, the specification has been found wanting. In the claims, the subject matter of encrypting and decrypting a value based on a secret that comprises the order of a Jacobian of a curve is not enabled because the breath of the claims is much greater than the enabling disclosure of the invention. MPEP 2164.01(a).

9. On pg. 18, 1st paragraph of the Remarks, Applicant argues that the 101 rejections to claims 40-47 are improper since the claims are directed to a system including multiple modules and fails to see how the recited claims are not tangible; to clarify: the specification identifies an embodiment wherein the multiple modules are not

limited to tangible embodiments. Specification, pg. 14, 3rd full paragraph. Hence, the claims are not solely directed to statutory subject matter.

10. Applicant's arguments, see Remarks, pgs: 18-19, with respect to the 102 and 103 rejections of claims 11, 17 and 20-47 have been fully considered and are persuasive. The prior art of record discloses using key exchange to encrypt a message transmission by means of Diffie-Hellman or ElGamal using a group including the jacobian of a hyperelliptic curve defined over a finite field, as well as an elliptic curve analogue to DSA (Koblitz, pgs. 132-136; pg. 148, section 6). The values necessarily made public by the entity to encrypt the message is the generator (alpha) of the cyclic group (G); the group element (alpha^a), where a is a random value between 1 and n-1 (n is the order of Group G); and the value n. Also the values necessarily made public by the entity generating a signature include the order of the group (Koblitz, pgs. 134-136, section 2.4 Digital Signature). Claims 11, 13, 17 and 20-47, in contrast, cover maintaining the order of a group as a secret; hence, the 102 and 103 rejections of these claims are withdrawn.

11. With respect to the 103 rejections of claims 1-10, 12-16, 18 and 19, Applicant's allegations that the prior art does not disclose the limitation of converting the number to an element of the Jacobian curve and raising the element to a particular power (see claim 1), or raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on an element of a Jacobian

of a curve (see claim 14) (Remarks, pgs. 20-22), are not founded. Elliptic curve signature generation and verification based on DSA requires an element of the Jacobian of a curve and raises the element to a particular power to generate the signature, and raising a value to an particular exponent to obtain a resulting value, wherein the raising is based at least in part on an element of a Jacobian of a curve (Koblitz, pgs. 134-135, section 2.4 Digital Signature). Hence, the prior art of record cover the limitations of these claims.

Claim Rejections - 35 USC § 112

12. Claims 20-22, 24-28, 30-37, 39-43, 45 and 46 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for receiving a value; padding the received value using a recognizable pattern; converting the padded value to a number represented by a particular number of bits; converting the padded value to a number represented by a particular number of bits; converting the number to an element of the Jacobian of a curve; raising the element to a particular power; compressing the result of raising the element to the particular power; and outputting, as the product identifier, the compressed result; wherein the conversion of the number to an element of the Jacobian of the curve is based at least in part on an order of a group of points on the Jacobian of the curve, and wherein the order of the group of points on the Jacobian of the curve is maintained as a secret (see specification, pgs. 13-14 and 18-19), does not reasonably provide enablement for all encrypting or decrypting techniques on a message based on a secret that is the order of a group of points on a

Jacobian. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these claims. The breath of the limitation of encrypting or decrypting a message based on a secret that is the order of a group of points on the Jacobian, is much broader than that which is enabled by applicant's disclosure.

13. Claims 1-10, 12-16 and 18-19 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. Regarding claims 1-10, 12 and 13, the omitted structural cooperative relationships are: the conversion of the number to an element of the Jacobian of the curve is based at least in part on an order of a group of points on the Jacobian of the curve, and wherein the order of the group of points on the Jacobian of the curve is maintained as a secret (see claim 11); and regarding claims 14-16, 18 and 19, the omitted structural cooperative relationships are: the raising is further based at least in part on an order of a group of points on the Jacobian of the curve, and wherein the order of the group of points on the Jacobian of the curve is maintained as a secret (see claim 17). These relations are essential to the respective claims because the security of the invention depends on the secrecy of the order of the group of points on the Jacobian of the curve. Specification, pg. 13, last paragraph.

Claim Rejections - 35 USC § 101

14. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 40-47 are rejected under 35 U.S.C. 101 as not being tangible. In view of Applicant's disclosure, specification pg. 14, 3rd full paragraph, the medium is not limited to tangible embodiments, instead they are defined as including both tangible embodiments (e.g., hardware) and intangible embodiments (e.g., software). As such, the claims are not limited to statutory subject matter and are therefore non-statutory.

Claim Rejections - 35 USC § 103

15. Claims 1-10, 12, 14-16, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koblitz in view of Schneier Applied Cryptography (hereinafter Schneier) and Blumenau et al. U.S. Patent No. 6,845,395 (hereinafter Blumenau).

16. As per claims 1, 2 and 5-10 and 12, Koblitz discloses a discrete log cryptosystem, wherein a value is converted into an element of the Jacobian of a curve, raising the element to a particular power, and this conversion is based at least in part on an order of a group of points on the Jacobian of the curve, wherein the curve comprises a hyperelliptic curve, wherein the curve is given by the equation of y^2=f(x), wherein f(x) has a degree of 2g + 1, and wherein g refers to the genus of the curve; which further covers the step of converting the number to an element of the Jacobian of a curve.

Koblitz, pgs. 131-136, section 2, "Elliptic Curve Cryptosystems", pgs. 148-153, section 6, "Hyperelliptic Cryptosystems". This conversion has the property of masking the original value of a received value.

17. Koblitz does not expressly teach taking a received value, padding the received value using a recognizable pattern, converting the padded value to a number using a recognizable pattern, wherein converting the padded value to a number represented by a particular number of bits comprises defining a plurality of functions, wherein each of the plurality of functions returns a value that is a set of bits of a hash value generated based on an input value; further, separating the padded value into a plurality of portions and using the plurality of portions as input values for the plurality of functions, wherein each of the plurality of functions returns a set of least significant bits of a hash value generated based on the input, wherein the hash value is generated using a secure hashing process, wherein the set of bits includes a number of bits equal to half the particular number of bits, and wherein the separating comprises separating the padded value into two equal portions. Schneier discloses using MD5 and SHA hashing algorithms to distill a condense unique value from an original value, wherein this unique value effectively identifies the original value. Operations of this type enable functions to operate on hashed values rather than the corresponding original and larger values to create values linked to the hashed value and by extension to the original value. Further, received values are typically padded as multiples of a number 2^n prior to hashing. In the case of SHA or MD5, n=9. Schneier, pgs 442-445, section 18.7, 'Secure Hash Algorithm'. Hence, it would be obvious to one of ordinary skill in the art at the time the

invention was made to hash a received value prior to converting the number to an element of a Jacobian curve since it enables the method to take arbitrary-length values and create a fixed length string for computation, which facilitates more efficient processing. Schneier, pg. 429, section 18.1, 'Background'.

18. Koblitz does not expressly teach compressing the resulting element and outputting the result. However, it is well known in the art to use compression techniques on data such that the data comprises less information but has the reversible property of being decompressed to the original data. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to compress the resulting value since compressed data has desirable properties including encoding data to a set length to further enhance processing value of the data as known to one of ordinary skill.

19. Finally, Koblitz does not teach using the aforementioned steps to generate a product identifier. Blumenau discloses encrypting an identifier to prevent other devices from using the identifier and gaining access to services. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate a product identifier using the steps taught by Koblitz since product identifiers need to be secured to prevent other devices from using the identifier and gaining access to services. Blumenau, col. 11:55-61. The aforementioned cover the limitations of claims 1, 2 and 5-10 and 12.

20. As per claim 3, the rejections of claims 1, 2, 5-10 and 12 under 35 U.S.C. 103(a) are incorporated herein. (supra) Although Schneier only teaches padding the received value with zeros, any padding comprising a pattern such that the hash value can be replicated to verify the integrity of a hash is an obvious variation-the portion of the received value is readily available as a padding value. Further, it is notoriously well known to extend the value of a message with any regular pattern up to a fixed multiple as required by methods that process data in blocks. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the recognizable pattern to comprise at least a portion of the received value, since the received value is readily available as known to one of ordinary skill in the art.

21. As per claim 4, the rejection of claim 1 is incorporated herein. Koblitz does not teach converting the padded value to a 114-bit number. However, the conversion of a value padded to a specific length is typically consistent with the architecture of the underlying process or machine. For example, values output from one step and input to another step require length conversions such that the output value meets the required sized of the input. Hence, the conversion of the padded value to a 114 bit number is a matter of design choice. It would be obvious to one of ordinary skill in the art at the time the invention was made, wherein the padded value is converted to a 114 bit number since the size of the number is dependent on the required size of an input value of a function as known to one of ordinary skill in the art.

22. As per claims 14-16, 18 and 19, the rejections of claims 1-10 and 12 are incorporated herein. In addition, the encryption method of Koblitz has a corresponding decryption method. Hence, the aforementioned cover the limitations of claims 14-16, 18 and 19.

Allowable Subject Matter

23. Claims 11, 17, 23, 29 and 38 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

24. Claims 13, 20-22, 24-28, 30-37 and 39-47 are not covered by the prior art of record.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

August 9, 2005

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100